

Table of Contents

1. Elementary Number Theory	1
1.1 Introduction	1
1.1.1 What is Number Theory?	1
1.1.2 Algebraic Preliminaries	12
1.2 Theory of Divisibility	20
1.2.1 Basic Properties of Divisibility	20
1.2.2 Fundamental Theorem of Arithmetic	24
1.2.3 Mersenne Primes and Fermat Numbers	27
1.2.4 Euclid's Algorithm	32
1.2.5 Continued Fractions	36
1.3 Diophantine Equations	41
1.3.1 Basic Concepts of Diophantine Equations	41
1.3.2 Linear Diophantine Equations	42
1.3.3 Pell's Equations	45
1.4 Arithmetic Functions	50
1.4.1 Multiplicative Functions	50
1.4.2 Functions $\tau(n)$, $\sigma(n)$ and $s(n)$	51
1.4.3 Perfect, Amicable and Sociable Numbers	54
1.4.4 Functions $\phi(n)$, $\lambda(n)$ and $\mu(n)$	61
1.5 Distribution of Prime Numbers	64
1.5.1 Prime Distribution Function $\pi(x)$	65
1.5.2 Approximations of $\pi(x)$ by $x/\ln x$	67
1.5.3 Approximations of $\pi(x)$ by $\text{Li}(x)$	73
1.5.4 The Riemann ζ -Function $\zeta(s)$	74
1.5.5 The n th Prime	83
1.5.6 Distribution of Twin Primes	86
1.5.7 The Arithmetic Progression of Primes	89
1.6 Theory of Congruences	90
1.6.1 Basic Properties of Congruences	90
1.6.2 Modular Arithmetic	94
1.6.3 Linear Congruences	96
1.6.4 The Chinese Remainder Theorem	101
1.6.5 High-Order Congruences	104
1.6.6 Legendre and Jacobi Symbols	107

1.6.7	Orders and Primitive Roots	115
1.6.8	Indices and k th Power Residues	120
1.7	Arithmetic of Elliptic Curves	124
1.7.1	Basic Concepts of Elliptic Curves	125
1.7.2	Geometric Composition Laws of Elliptic Curves	128
1.7.3	Algebraic Computation Laws for Elliptic Curves	129
1.7.4	Group Laws on Elliptic Curves	133
1.7.5	Number of Points on Elliptic Curves	134
1.8	Bibliographic Notes and Further Reading	135
2.	Algorithmic Number Theory	139
2.1	Introduction	139
2.1.1	What is Algorithmic Number Theory?	139
2.1.2	Effective Computability	142
2.1.3	Computational Complexity	146
2.1.4	Complexity of Number-Theoretic Algorithms	153
2.1.5	Fast Modular Exponentiations	159
2.1.6	Fast Group Operations on Elliptic Curves	163
2.2	Algorithms for Primality Testing	167
2.2.1	Deterministic and Rigorous Primality Tests	167
2.2.2	Fermat's Pseudoprimalty Test	170
2.2.3	Strong Pseudoprimalty Test	173
2.2.4	Lucas Pseudoprimalty Test	179
2.2.5	Elliptic Curve Test	186
2.2.6	Historical Notes on Primality Testing	190
2.3	Algorithms for Integer Factorization	192
2.3.1	Complexity of Integer Factorization	192
2.3.2	Trial Division and Fermat Method	196
2.3.3	Legendre's Congruence	198
2.3.4	Continued FRAction Method (CFRAC)	201
2.3.5	Quadratic and Number Field Sieves (QS/NFS)	204
2.3.6	Pollard's " <i>rho</i> " and " $p - 1$ " Methods	208
2.3.7	Lenstra's Elliptic Curve Method (ECM)	215
2.4	Algorithms for Discrete Logarithms	218
2.4.1	Shanks' Baby-Step Giant-Step Algorithm	219
2.4.2	Silver-Pohlig-Hellman Algorithm	222
2.4.3	Subexponential Algorithms	226
2.4.4	Algorithm for the Root Finding Problem	227
2.5	Quantum Number-Theoretic Algorithms	230
2.5.1	Quantum Information and Computation	230
2.5.2	Quantum Computability and Complexity	235
2.5.3	Quantum Algorithm for Integer Factorization	236
2.5.4	Quantum Algorithms for Discrete Logarithms	241
2.6	Miscellaneous Algorithms in Number Theory	243
2.6.1	Algorithms for Computing $\pi(x)$	243

2.6.2	Algorithms for Generating Amicable Pairs	249
2.6.3	Algorithms for Verifying Goldbach's Conjecture	252
2.6.4	Algorithm for Finding Odd Perfect Numbers	255
2.7	Bibliographic Notes and Further Reading	257
3.	Applied Number Theory	259
3.1	Why Applied Number Theory?	259
3.2	Computer Systems Design	261
3.2.1	Representing Numbers in Residue Number Systems	261
3.2.2	Fast Computations in Residue Number Systems	264
3.2.3	Residue Computers	269
3.2.4	Complementary Arithmetic	269
3.2.5	Hashing Functions	273
3.2.6	Error Detection and Correction Methods	277
3.2.7	Random Number Generation	282
3.3	Cryptography and Information Security	287
3.3.1	Introduction	288
3.3.2	Secret-Key Cryptography	289
3.3.3	Data/Advanced Encryption Standard (DES/AES)	299
3.3.4	Public-Key Cryptography	303
3.3.5	Discrete Logarithm Based Cryptosystems	309
3.3.6	RSA Public-Key Cryptosystem	313
3.3.7	Quadratic Residuosity Cryptosystems	326
3.3.8	Elliptic Curve Public-Key Cryptosystems	332
3.3.9	Digital Signatures	336
3.3.10	Digital Signature Algorithm/Standard (DSA/DSS)	342
3.3.11	Database Security	344
3.3.12	Secret Sharing	348
3.3.13	Internet/Web Security and Electronic Commerce	352
3.3.14	Steganography	356
3.3.15	Quantum Cryptography	358
3.4	Bibliographic Notes and Further Reading	359
	Bibliography	363
	Index	375